

**MORRIS, JAMES, HITCHENS & WILLIAMS LLP**

222 Delaware Avenue, 10th Floor  
Wilmington, Delaware 19801-1621  
(302) 888-6800  
Facsimile (302) 571-1750  
www.morrisjames.com

Richard K. Herrmann  
(302) 888-6816  
rherrmann@morrisjames.com

Mailing Address  
P.O. Box 2306  
Wilmington, DE 19899-2306

September 14, 2006

**VIA E-FILING AND HAND DELIVERY**

The Honorable Sue L. Robinson  
United States District Court  
District of Delaware  
844 King Street  
Wilmington, DE 19801

**Re: *SRI International v. ISS and Symantec*, D. Del., C.A. No. 04-1199-SLR**

Your Honor:

I write in response to SRI's letter to the Court dated September 8 regarding SRI's withdrawal of its claim that Symantec infringes U.S. Patent No. 6,321,338.

Symantec has requested that SRI confirm that it will not assert the claims of the '338 patent in the future against Symantec or its customers based upon any past or present Symantec product. Assuming that SRI provides that representation, Symantec is hopeful that the parties will resolve this issue without the need for the Court's assistance.

Should SRI's infringement claim be properly disposed, it is not accurate, as SRI suggests, that "much of Symantec's pending motion for summary judgment of non-infringement" is mooted. Three of the four arguments presented in Symantec's motion are not directed towards the '338 patent at all, but rather the three other patents-in-suit, including Symantec's argument that SRI has failed to identify any instance in which Symantec's "SGS" and "Manager" products are combined together in an infringing manner.

In the meantime, the U.S. Patent and Trademark Office ("PTO") issued another order relevant to Defendants' pending motion for summary judgment of invalidity. On September 5, 2006, the PTO granted a request for *ex parte* reexamination of the '338 patent. [Ex. A]. This Order finds in part that one of the references relied upon in Defendants' pending summary judgment motion for invalidity - the JiNao Report - was not previously considered by the PTO and raises a substantial new question of patentability with respect to all of the claims of the '338 patent.

MORRIS, JAMES, HITCHENS & WILLIAMS LLP

The Hon. Sue L. Robinson  
September 14, 2006  
Page 2

As noted previously, the PTO has also granted a request for ex parte reexamination of United States Patent No. 6,484,203. Requests for re-examination of the remaining patents-in-suit are also pending before the PTO. Symantec will inform the Court if there are any material developments relating to those reexamination requests.

Respectfully,

A handwritten signature in black ink, appearing to be 'RKH' with a long horizontal stroke extending to the right.

Richard K. Herrmann

Enclosure

cc: John Horvath, Esq. (via email w/ enclosure)  
David Moore, Esq. (via email w/ enclosure)  
Katherine Prescott, Esq. (via email w/ enclosure)  
Theresa Moehlman, Esq. (via email w/ enclosure)  
Holmes Hawkins, III, Esq. (via email w/ enclosure)

# **EXHIBIT A**



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**DO NOT USE IN PALM PRINTER**

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Day Casebeer Madrid & Batchelder LLP  
Attn: Renee DuBord Brown, Esq.  
20300 Stevens Creek Blvd., Suite 400  
Cupertino, CA 95014

**EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. 90/008,123.

PATENT NO. 6321338.

ART UNIT 3992.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/008,123	07/07/2006	6321338	1904-001	3409

7590 09/05/2006

DAVID L FEIGENBAUM  
 FISH AND RICHARDSON  
 225 FRANKLIN STREET  
 BOSTON, MA 02110-2804

EXAMINER

ART UNIT

PAPER NUMBER

DATE MAILED: 09/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Order Granting / Denying Request For Ex Parte Reexamination</b>	<b>Control No.</b>	<b>Patent Under Reexamination</b>	
	90/008,123	6321338	
	<b>Examiner</b>	<b>Art Unit</b>	
	Roland G. Foster	3992	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed 07 July 2006 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a) ☐ PTO-892, b) ☒ PTO/SB/08, c) ☒ Other: See the attached Decision

1. ☒ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**


For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

2. ☐ The request for *ex parte* reexamination is DENIED.

This decision is not appealable (35 U.S.C. 303(c)). Requester may seek review by petition to the Commissioner under 37 CFR 1.181 within ONE MONTH from the mailing date of this communication (37 CFR 1.515(c)). **EXTENSION OF TIME TO FILE SUCH A PETITION UNDER 37 CFR 1.181 ARE AVAILABLE ONLY BY PETITION TO SUSPEND OR WAIVE THE REGULATIONS UNDER 37 CFR 1.183.**

In due course, a refund under 37 CFR 1.26 ( c ) will be made to requester:

- a) ☐ by Treasury check or,  
b) ☐ by credit to Deposit Account No. \_\_\_\_\_, or  
c) ☐ by credit to a credit card account, unless otherwise notified (35 U.S.C. 303(c)).

  
Roland G. Foster  
Primary Examiner  
Art Unit: 3992

cc:Requester ( if third party requester )  
U.S. Patent and Trademark Office  
PTOL-471 (Rev. 08-06)

Office Action In *Ex Parte* Reexamination

Part of Paper No. 20060901

Application/Control Number: 90/008,123  
Art Unit: 3992

Page 2

### DECISION

A substantial new question of patentability affecting claims 1-27 of United States Patent Number 6,321,338 B1 (the "Porras" patent) is raised by the request for *ex parte* reexamination, filed on July 7, 2006 (the "Request").

Pages 2-5 of the Request identify the following printed publications as providing teachings relevant to the claims of the Porras patent:

1. D. Anderson, T. Frivold, and A. Valdes, Next-generation Intrusion Detection Expert System (NIDES) A Summary, Computer Science Laboratory, SRI-CSL-95-07, May 1995 ("Network NIDES")
2. Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure*, Technical Report, DARPA Order No. E296, Contract No. F30602-96-C0325, April 1997 ("JiNao Report").
3. L. Todd Heberlein et al., *A Network Security Monitor*, 1990 IEEE Computer Society Symposium on Research in Security and Privacy, May 1990 ("NSM 1990").
4. Feather, Frank Edward, Ph.D. *Fault detection in an Ethernet network via anomaly detectors*, Carnegie Mellon University, 1998 ("Feather Thesis")

A reasonable examiner would consider the above prior references important in making a decision as to the patentability of claims 1-27 of the Porras patent.

Application/Control Number: 90/008,123

Page 3

Art Unit: 3992

Identification of Every Claim for Which Reexamination is Requested

The above-cited publications (Network NIDES, JiNao Report, NSM 1990, and the Feather Thesis) are separately discussed regarding claims 1-27 of the Porras patent. See pages 9-42 of the Request and exhibits B, C, D, E, and F.

Statement Pointing Out Each Substantial New Question of Patentability

The teaching in each cited prior art document that provides a basis for each substantial new question of patentability is separately discussed. See the claim charts (page 9-42) in the Request and exhibits B, C, D, E, and F, which point out the teachings in each of the above-cited publications. The Request also states that the above-cited references were never cited during prosecution of the Porras patent. Thus, each substantial new question raised in the request is a new question.

Detailed Explanation of How the Cited Prior Art is Applied to Every Claim for Which  
Reexamination is Requested

The above-cited publications (Network NIDES, JiNao Report, NSM 1990, and the Feather Thesis) are separately discussed regarding how they apply to claims 1-27 of the Porras patent. See page 9-42 of the Request regarding claim charts that apply independent claim 1 to each of the above-mentioned publications. Independent claim 21 is discussed as being



Application/Control Number: 90/008,123

Page 4

Art Unit: 3992

substantively similar to claim 1, as discussed on page 6 of the Request. See page 6 of the Request and exhibits B, C, D, and E regarding the dependent claims. Exhibits B, C, D, and E also explain which claim limitations are subject to 103 rejections, where Exhibits F and G explain what teachings from various secondary references are applied to these limitations. Thus, the Request clearly explains how the cited combination is applied to the limitations of a particular claim.

#### Network NIDES

A reasonable examiner would consider the Network NIDES reference important in making a decision as to the patentability of claims 1-27 of the Porras patent. Claim 1, which is representative, recites:

**A method of network surveillance, comprising:**

**receiving network packets handled by a network entity;**

**building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;**

**comparing at least one long-term and at least one short-term statistical profile; and**

**determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.**

The Network NIDES reference teaches of applying intrusion-detection technology to a network computer environment that reads network packets (receiving network packets handled by a network entity), generating a long-term and short-term file of statistical information

Application/Control Number: 90/008,123

Page 5

Art Unit: 3992

(building at least one long-term and at least one short-term statistical profile) based on network conditions, such as the amount of traffic originating or being received by local and remote hosts, refused connections, etc. (monitoring data transfers, errors, or network connections), raising an alarm when observed activity departs from established patterns of use (determining whether the difference indicates suspicious network activity). For additional details, see the claim chart set forth on pages 10 – 14 of the Request.

A question has also been raised as to whether the Network NIDES reference is combinable with various other secondary references in order to teach limitations directed to methods for analyzing network traffic as recited in independent claims 1 and 12. See pages 14 - 17 of the Request and Exhibits B, F and G for additional details, which clearly explains how the various combinations are applied to the limitations of each particular claim.

The Network NIDES reference was not previously considered (as discussed above) nor addressed in the prior examination of the patent or a final holding of invalidity by the Federal Courts.

Thus, a reasonable examiner would consider the new teachings of Network NIDES important in deciding to allow the claims being considered.

Application/Control Number: 90/008,123  
Art Unit: 3992

Page 6

JiNao

A reasonable examiner would consider the JiNao Report important in making a decision as to the patentability of claims 1-27 of the Porras patent. With respect to claim 1, which is representative as discussed above, the JiNao Report teaches of targeting network traffic for purposes of detection (receiving network packets handled by a network entity), building a long-term and short-term probability distribution (building at least one long-term and at least one short-term statistical profile) based on network conditions, such as packet and LSA arrival frequencies, volume of general activity, and bursts of activity or prolonged activity that is abnormal (monitoring data transfers, errors, or network connections), comparing a subject's short-term behavior with the subject's historical or long-term behavior and raising a warning flag if the two are sufficiently unlike each other (determining whether the difference indicates suspicious network activity). For additional details, see the claim chart set forth on pages 19-23 of the Request.

A question has also been raised as to whether the JiNao Report is combinable with various other secondary references in order to teach limitations directed to methods for analyzing network traffic as recited in independent claims 1 and 12. See pages 25 -27 of the Request and Exhibits C, F and G for additional details, which clearly explains how the various combinations are applied to the limitations of each particular claim.

Application/Control Number: 90/008,123  
Art Unit: 3992

Page 7

The JiNao Report reference was not previously considered (as discussed above) nor addressed in the prior examination of the patent or a final holding of invalidity by the Federal Courts.

Thus, a reasonable examiner would consider the new teachings of JiNao Report important in deciding to allow the claims being considered.

NSM 1990 and the Feather Thesis

Similarly to the Network Nides and JiNao Report, the Request applies the NSM 1990 and Feather Thesis in a similar manner to the claims. See 28 - 41 of the Request, including the detailed claim charts and Exhibits D, E, F, and G. Neither were these references addressed in the prior examination of the Porras patent (as discussed above) or in a final holding of invalidity by the Federal Courts. Thus, a reasonable examiner would consider these publications important, alone or in combination with various secondary references, in making a decision as to the patentability of claims 1-27 of the Porras patent.

Application/Control Number: 90/008,123  
Art Unit: 3992

Page 8

### Conclusion

With respect to the Information Disclosure Statement ("IDS") filed on July 7, 2006, the IDS cites documents that do not meet the prior art, printed publication, and/or pertinency requirements and have therefore not been considered. Although some references cited on the IDS may have previously been considered during the initial examination, during a reexamination proceeding citation of documents for which no explanation of pertinency and applicability is provided, not to mention analysis regarding any SNQ, fail to meet the requirements set forth by 37 U.S.C. 1.501 and 37 U.S.C. 1.510(b)(2). Those references cited on the IDS that are not in compliance will be lined through by the examiner and not considered. See MPEP § 2202, 2205, and 2214.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the Hong patent throughout the course of this reexamination proceeding. The requester is also reminded of the ability to similarly appraise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Application/Control Number: 90/008,123

Page 9

Art Unit: 3992

Please mail any communications to:

Attn: Mail Stop "Ex Parte Reexam"  
Central Reexamination Unit  
Commissioner for Patents  
P. O. Box 1450  
Alexandria VA 22313-1450

Please FAX any communications to:

(571) 273-9900  
Central Reexamination Unit

Please hand-deliver any communications to:

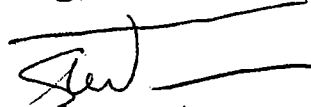

Customer Service Window  
Attn: Central Reexamination Unit  
Randolph Building, Lobby Level  
401 Dulany Street  
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:



Roland G. Foster  
Central Reexamination Unit, Primary Examiner  
Electrical Art Unit 3992  
(571) 272-7538

CONFERREES  
  
Scott L. Weaver  
AUCRU 3992  
  
MARK J. REINHART  
SPRE-AU 3992  
CENTRAL REEXAMINATION UNIT

PTO/SB/08B (07-05)

Approved for use through 07/31/2006, OMB 0651-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)


**Complete If Known**

Application Number	Not yet assigned 90/008,123
Filing Date	Not yet assigned
First Named Inventor	Phillip A. Porras
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	1904-001

Sheet 1 of 2

**NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
R.C.T.	A	D. ANDERSON, T. FRIVOLD, A. VALDES, Next-Generation Intrusion Detection Expert System (A Summary), SRI-CSL-95-07, May 1995.	
R.C.T.	B	Y. F. JOU, et al., Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure, Technical Report, April 1997.	
R.C.T.	C	L. T. HEBERLEIN, et al., A Network Security Monitor, 1990 IEEE Computer Society Symposium on Research in Security and Privacy, p. 296-304, IEEE Computer Society Press, 1990.	
R.C.T.	D	F. FEATHER, Fault detection in an Ethernet network via anomaly detectors, Carnegie Mellon University, 1992.	
R.C.T.	E	WHEELGROUP CORPORATION, NetRanger 1.3.1 User's Guide, 1997.	
R.C.T.	F	P. PORRAS, P. NEUMANN, EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, p. 353-365, 20th NISSC, Oct. 7-9, 1997.	
R.C.T.	G	S. SNAPP, et al., DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype, 14th National Computer Security Conference, p. 167-176, 1991.	
R.C.T.	H	SUN MICROSYSTEMS, SunScreen EFS Configuration and Management Guide, Release 1.1, Rev. A, June 1997.	
R.C.T.	I	J. CASE et al., A Simple Network Management Protocol (SNMP), Network Working Group, Request for Comments: 1157, May 1990.	
R.C.T.	J	M. ROSE, K. MCCLOUGHRIE, Structure and Identification of Management Information for TCP/IP-based Internets, Network Working Group, Request for Comments: 1155, May 1990.	

Examiner Signature		Date Considered	9/1/06
--------------------	---	-----------------	--------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (07-05)

Approved for use through 07/31/2006. OMB 0851-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

**Complete if Known**

Sheet 2 of 2

Application Number	Not yet assigned 90/008,123
Filing Date	Not yet assigned
First Named Inventor	Phillip A. Porras
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	1904-001

**NON PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
R.C.F.	K	K. MCCLOUGHRIE, M. ROSE, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, Network Working Group, Request for Comments: 1213, March 1991.	
R.C.F.	L	S. WALDBUSSER, Remote Network Monitoring Management Information Base, Network Working Group, Request for Comments: 1271, Nov. 1991.	
	M	S. WALDBUSSER, Remote Network Monitoring Management Information Base, Version 2 using SMIv2, Network Working Group, Request for Comments: 2024, Jan. 1997.	
	N	D. PERKINS & E. MCGINNIS, Understanding SNMP MIBs, 1997.	
R.C.F.	O	W. STALLINGS, SNMP, SNMPv2 and CMIP, The Practical Guide to Network-Management Standards, 1993.	
	P	M. MILLER, Managing Internetworks with SNMP, Second Ed., M&T Books, New York, New York, 1997.	
	Q	S. GARFINKEL, G. SPAFFORD, Practical UNIX & Internet Security, 2nd Ed., O'Reilly & Assoc., 1996.	
	R	D.B. CHAPMAN, E. ZWICKY, Building Internet Firewalls, 1st Ed., O'Reilly & Assoc., 1995.	
	S	A. VALDES, D. ANDERSON, Statistical methods for Computer Usage Anomaly Detection Using NIDES, Third International Workshop on Rough Sets and Soft Computing, 1995.	
	T	P. PORRAS, A. VALDES, Live Traffic Analysis of TCP/IP Gateways, 1998 ISOC Symposium on Network and Distributed Systems Security, 1998.	

Examiner Signature	<i>[Signature]</i>	Date Considered	9/1/06
--------------------	--------------------	-----------------	--------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.